USACE Finance Center
Corps of Engineers Financial Management System
(CEFMS)
Y2K Risk Assessment
1 Dec 1998

The Year 2000, (Y2K) is a serious issue that may have critical implications if not properly addressed. The USACE Finance Center is committed to ensuring Y2K compliance, preventing Y2K problems and developing a strategy for risk management. One of the USACE Finance Center's top priorities is Y2K date compliance for all of the supporting systems and their interfaces. This plan includes Y2K risks associated to financial information and other information technology outside the traditional financial information area, such as infrastructure systems and equipment.

All USACE Finance Center managers are fully aware of Year 2000 issues and are being continuously informed and guided as the compliance approach is implemented. We are committed to the Plan that was developed in accordance with the General Accounting Office (GAO) guidelines on the Year 2000 compliance process. In partnership with the USACE Information Management Office Year2000 Team and under the direction of the Finance Center Directorate, the CEFMS Financial Maintenance and Development Directorate is providing planning, guidance, management oversight, and technical support and has the ultimate responsibility to develop and execute Year 2000 compliance plans for Y2K risks associated with the Corps of Engineers Financial Management System.

The Department of Army designated CEFMS as mission critical. This implies that USACE must provide formal compliance reporting and certification to the Department of the Army. One of these requirements is a formal Risk Assessment Plan.

The CEFMS Y2K Risk Assessment provides for identifying and implementing preventative maintenance, controlling the residual risks and minimizing interruption of business operations that may be experienced by users of CEFMS, or other enterprise Interfacing/Integrated systems. System functionality that is not dependent or interdependent with financial data may not be within the scope of this document. We believe the key to a successful transition into the Year2000 millenium is dependent upon coordination and communication among all Corps/DOD AIS Project teams.

I. **Strategic Components**

I. **Purpose:**

This risk assessment is designed to protect the assets and continuity of financial management and business operations of organizations by reducing the potential threat of loss of automated methods to manage financial operations before they may occur. Potential Y2K risks includes catastrophic loss, such as natural disasters, and human error. Our staff is committed to continuous monitoring and assessing existing and potential exposures as the new millenium approaches.

2. Organization and methods

The objectives are to resolve risk through preventative measures. One important element of our risk management strategy is the communication of risk management benefits to all organizations. We believe this is an essential ingredient to the Corps' success in developing an integrated and comprehensive risk management strategy.

3. Overview: A summary of risk assessment is provided below.

II. Strategy

Policy: Defines the Y2K strategy of the resolution phase.

Organization: Roles and responsibilities:

The person in charge assesses the potential risks and develops or updates plans, assigns personnel to handle different tasks and ensures that those people are adequately trained. This individual should be familiar with the potential risks of all operations throughout the system and facility. In an emergency situation, the person in charge directs the Y2K resumption team. The Corps Continuation of Operations Plan will be implemented by appropriate functionals where applicable.

Approach: The basis for this proactive, quantitative, integrated, and systematic approach includes developing awareness, auditing potential weaknesses and creating an inventory, assessing exposures, assigning priorities, developing remedial plans, develop contingency plans, implementing corrective actions, and continuous testing for Compliance

III. Process

Risk: Process for identifying and assessing risks:
- Identify Risk or potential exposure
- Evaluate and analyze identified exposures
- Risk control of exposures through elimination and/or reduction
- Address contingency financing for potential unidentified exposures
- Develop an Y2K Resumption team capable of responding to an emergency within a wide range of potential crises. The Y2K resumption team must respond quickly and without confusion, fear or panic. The team shall consist of members who clearly understand their responsibilities and who are fully trained to carry them out in an emergency.

Contingency planning: Approaches and preferred alternatives for handling risk are addressed in the Y2K Contingency Plan.

IV. Verification

Risks:

- **Hardware:**

BIOS problems in PC's and Servers - PC workstations and/or servers may be non-Y2K compliant. When they are set to December 31, 1999, and then turned off, once restarted later they may have the wrong system date (1980 or 1984 instead of 2000) or may shut themselves down. The problem occurs in how the chip called the "BIOS" interacts with the "Real Time Clock".

Estimated Level of Risk:

Catastrophic Critical Marginal Negligible X None

Alternatives: Currently CEFMS does not utilize pc internal clocks to process data.

Resource Requirements & Implications: None

Priority: Low, dependent upon site evaluations.

Actions to Mitigate Risk: Implement a Corps wide Y2K Pc Test plan.

Relationship to other information resources & other business-functions: Should an interfacing and/or integrating system utilize a pc internal clock for I/O processing where the pc is non-Y2K compliant the data would require correction prior to transfer to/from CEFMS.

Preventative Measures - An automated Y2K testing tool was utilized to evaluate and correct each USACE Finance Center PC. Each site manager is responsible for ensuring his or her equipment is Y2K compliant. Sites that fail to secure sufficient Y2K compliant equipment should not be affected directly from CEFMS I/O. However, if they utilize external systems or software for preliminary or post financial analysis their continued operations may be hindered pending a resolution for their specific problem.

- **Operating System (OS) level:**

Operating systems - It has been detected that some versions of the unix operating system will have a problem with year 2000 because of the way the internal date is stored. Currently the supporting Unix operating system utilized for CEFMS is SOLARIS 2.5.1 which is not Y2K certified by it's vendor.

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible None

Alternatives: Update the version of Unix or implement a series of patches to correct the problem.

Resource Requirements & Implications: Resources are currently available to implement this change. Coordination with other functionals, such as the CEAP Centers, is required to complete the upgrade.

Priority: High as this problem is a show stopper if not corrected prior to 1 Jan, 2000.

Actions to Mitigate Risk: Upgrade the existing version of Unix.

Preventative Measures - An upgrade to a Y2K compliant Unix Operating System version is in progress. The upgrade is scheduled for completion prior to 1 Jan, 2000.

- **Telecommunications systems:** Mail Systems, routers, bridges, gateways, and so on, of the network configuration - (Local Area Network/Wide Area Network)

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible None

Alternatives: Our current local area network and email system is furnished by other Corps resources. Therefore we are reliant on their certification that these systems are Y2K compliant to ensure no disruption of service.

Resource Requirements & Implications:

Priority: High as this service is deemed crucial for uninterrupted service.

Actions to Mitigate Risk: Systems providing services to organizations outside their FOA, field operating activity, should provide Y2K certification to their customers. The CEAP Centers are responsible for wide are network communications.

- **External Databases and other spreadsheets:** Currently CEFMS databases are configured alike and reside on similar platforms. However, a risk may occur if end users utilize external software to continue or pre-process CEFMS I/O.

Estimated Level of Risk:
Catastrophic Critical Marginal Negligible X None

Alternatives: Users should test external software prior to processing CEFMS data for Y2K compliance to negate impacts.

Resource Requirements & Implications: None

Priority: Low, not mission critical

Actions to Mitigate Risk: Users should minimize utilization of external software in processing CEFMS data in order to preclude Y2K problems.

- **Custom software:** The CEFMS system is customized software and continuation of mission critical financial data is dependent upon successful transition to Y2K compliance.

Estimated Level of Risk:
Catastrophic X Critical Marginal Negligible None

Alternatives: The only alternative is manual processing. This is not a valid option for real time financial data processing which is part of the mission of the system.

Resource Requirements & Implications: Manpower requirements would be required.

Priority: High - Mission Critical

Actions to Mitigate Risk: Certify CEFMS Y2K compliant and coordinate with other interfacing/integrating vendor's to ensure a successful transition.

- **Data Problems including Interfaced/Integrated data:** The integrity of CEFMS, interfaced and integrated data is crucial to accurate financial transaction processing and reporting.

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible None

Alternatives: Utilize the current problem reporting process to address problem areas.

Resource Requirements & Implications: These requirements are dependent upon the severity of the problem encountered.

Priority: High priority should be assigned for Y2K problems to ensure continued service to all customers and enterprise systems.

Actions to Mitigate Risk: Certification from all AIS would reduce the potential for Y2K errors in processing data.

- **Software date calculations:** The renovation steps were completed and included accessing date calculations within CEFMS.

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible None

Alternatives: A correction to date processing may be implemented after careful review, analysis and coordination.

Resource Requirements & Implications: The degree of error would impact the requirements to implement a corrective action.

Priority: High, date errors should be corrected immediately to preclude negative impact to other AIS.

Actions to Mitigate Risk: Y2K date conversions have been implemented in CEFMS. Coordination with all known interfacing/integrating systems has been conducted. Interfacing/integrating systems have signed memorandums of agreement for Y2K compliance requirements.

- **Sorting in wrong order:** Sorting data by date is common practice in CEFMS and other AIS's.

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible None

Alternatives: Incorrect sorting may be corrected through the standard problem reporting processes. However, all dates have been made Y2K compliant in CEFMS and sorting has been tested.

Resource Requirements & Implications: The degree of error would impact the requirements to implement a corrective action.

Priority: High, correct dates are critical to accuracy of financial accounting data.

Actions to Mitigate Risk: Review and Certification from all AIS would reduce the potential for Y2K errors in sorting dates correctly.

- **Data problems for external applications:**

Estimated Level of Risk:
Catastrophic Critical Marginal X Negligible None

Alternatives: Users should test external software prior to processing CEFMS data for Y2K compliance to negate impacts.

Resource Requirements & Implications: None

Priority: Low, not mission critical

Actions to Mitigate Risk: Users should test external software for Y2k prior to processing I/O of financial data to preclude Y2K problems.

- **Software date calculations:**

Estimated Level of Risk:
Catastrophic X Critical Marginal Negligible None

Alternatives: A correction to date processing may be implemented after careful review, analysis and coordination.

Resource Requirements & Implications: The degree of error would impact the requirements to implement a corrective action.

Priority: High, correct dates are critical to accuracy of financial accounting data.

Actions to Mitigate Risk: Review and Certification from all AIS would reduce the potential for Y2K errors in I/O of dates.

Input Years as 2 Digits:

Estimated Level of Risk:
Catastrophic X Critical Marginal Negligible None

Alternatives: 2 digit dates may be utilized when Y2K impacts are analyzed and implemented prior to implementation.

Resource Requirements & Implications: The degree of error would impact the requirements to implement a corrective action.

Priority: High, correct dates are critical to accuracy of financial accounting data.

Actions to Mitigate Risk: Review and Certification from all AIS would reduce the potential for Y2K errors in I/O of 2 digit dates. 2 digit dates should be discouraged where feasible in all AIS.

- **Leap Year Rules:**

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible None

Alternatives: Leap years must be analyzed and a plan implemented prior to the new millenium.

Resource Requirements & Implications: The occurrences of errors would impact the requirements to implement a corrective action.

Priority: High, correct dates are critical to accuracy of financial accounting data.

Actions to Mitigate Risk: Review and Certification from all AIS would reduce the potential for Y2K errors in I/O of leap years. Coordination and communication among all AIS is critical in addressing peculiarities of leap years.

- **Embedded chip problems:** No embedded chip errors have been detected. However, this area is of concern as external tools and devices, for example facility alarms, are required to ensure uninterrupted services.

Estimated Level of Risk:
Catastrophic Critical Marginal X Negligible

Alternatives: None

Resource Requirements & Implications:

Priority:

- **Fixing custom code**: All code has been evaluated and corrected to be Y2K compliant.

Estimated Level of Risk:
Catastrophic Critical X Marginal Negligible
None

Alternatives: CEFMS code has been analyzed and upgraded prior to Y2K.

Resource Requirements & Implications: Implement corrective actions through source code modification utilizing the problem reporting system to monitor progress.

Priority: High, correct dates are critical to accuracy of financial accounting data.

Actions to Mitigate Risk: Review and Certification from all AIS would reduce the risk.

2. Tactical Components

Tactical Risk Management Plan for "Creeping Requirements"

Our analysis found that the average requirements overrun on our projects is minimal. We need to control creeping requirements to prevent uncontrolled cost.

In general, we looked for ways to eliminate the source of requirement changes by base lining the requirements. After that, we verified that only those requirement changes that are absolutely necessary were added to the baseline.

We are addressing the risk in three specific ways:

1. We're using a user interface prototype at the beginning of the project to be sure we gather high-quality requirements. We will continue showing the prototype to the users, refining it, and showing the prototype to the users again until we are confident that they will be very happy with the software we build.

2. We're placing the requirements specification under explicit change control. After we complete the user interface prototype and gather other requirements, we'll baseline the requirements. After that, requirement changes will have to go through a more formal change process in which cost, schedule, quality and other impacts have to be carefully assessed before the change is accepted.

3. We're using a staged delivery approach implementing steps. Between stages we can change features as required. We'll upgrade this risk to a higher level if the change requirements constitutes new functionality in the system or stops transaction processing. The functional lead is responsible for interfaces. The review change board is responsible for maintaining the requirements under change control. The Y2K Team Leader is responsible for keeping the stages within our staged delivery plan on track.

We'd like to have the Y2K baseline complete and beta tested by December 1998. If it isn't complete by this date, we'll upgrade the severity of this risk.

We estimated the Y2K renovation and testing cost. Explicit change control is accounted for in our standard development practices and does not add cost to the project. Y2K implementation increases the apparent project cost because of the increased effort associated with releasing the software upgrades in bulk.

3. **Preventative Maintenance Implementation:**

Implementation Steps:

1. Add new Year 2000 fields to CEFMS tables and views.

2. Create database triggers to keep both new Year 2000 fields and the fields which these new fields are replacing in sync.

3. Update tables where the new fields are added and set the current field equal to itself to fire the database triggers and populate the new Year 2000 fields.

4. Create NOT NULL check constraint on the new Year 2000 field if the current field cannot be null.

5. If current field is part of an index but not part of primary key, determine whether another index using the new Year 2000 field should be created.

6. If current field is part of the primary index, determine whether a supporting index on the new Year 2000 field should be created to maintain performance.

7. Modify problem report check-in programs to ensure that code changed is Year 2000 compliant.

8. Move changes 1 through 6 to all production sites.

9. Insure database triggers moved to production sites are working.

10. Identify and change all non-report programs to use the new Year 2000 fields.

11. Test all non-report programs changed in step 10 and move to all production sites.

12. Identify and change all report tables and programs to have and use new Year 2000 data elements.

13. Test all report tables and programs changed is step 12 and move to production sites.

14. Identify all non-report tables/current field/new year 2000 field and provide to production sites. Advise production sites to change local programs to use new year 2000 fields because the current fields will be removed from the CEFMS database.

15. Coordinate year 2000 changes with systems which interface with and/or share CEFMS data. Also, provide information identified in step 14 to the Points of Contacts for these systems.

16. Review/modify all ESIG stored procedures to in- sure all are year 2000 compliant.

17. Review all remaining CEFMS programs which have not been marked year 2000 compliant to insure no changes are needed and then mark as compliant.

18. After all programs are year 2000 compliant:

A. Drop indexes created in steps 5 and 6 that are no longer needed.
B. Recreate any constraints using old fields to use year 2000 fields.
C. Create database triggers to prevent old fields from being populated.
D. Remove old fields from the database.

5. Assessment Summary:

Initial implementation activities have been completed. Compliance Assessment and validation/ testing will be completed by December 1998.

The UFC Web site provides a means for sharing project information, status, results, coordination, and links to other Year 2000 sites. Our primary objective is to ensure the continuation of uninterrupted delivery of high quality financial management services to our customers. Our staff shall continually monitor and assess existing and potential exposures as the new millenium approaches.

signed 15 DEC 1998
STANLEY N. WRENN
Director USACE Finance Center